**Cyber Security Advisories**

**Date: 30 November 2024**

**Name of Control Centre:**

| **S No** | **Vulnerability Note No** | **Applicable to Organisation** | **If Yes: Action Taken:** | **Remarks** |
| --- | --- | --- | --- | --- |
| **(Yes/No)** | **Yes / No/ Deferred** |
|  | CMTX-P-112024264 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-290112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P112024074 A critical unauthenticated RCE vulnerability in the Palo Alto PAN-OS management interface |  |  |  |
|  | CMTX-I-993112024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-I-295112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P-112024794 Cumulative Suspicious Domains--ALERT2 |  |  |  |
|  | CMTX-P-112024274 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024284 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-401112024 ActionRAT Malware- Threat Actor: SideCopy |  |  |  |
|  | CMTX-P-112024074 PXA Stealer |  |  |  |
|  | CMTX-I-281112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-053112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-I-257112024 Malicious Domains used by Threat Actors |  |  |  |
|  | CMTX-P112024994 Relay server Nodes used by Chinese actors--ALERT11 |  |  |  |
|  | CMTX-P-112024038 Critical Alert: Helldown Ransomware |  |  |  |
|  | CMTX-P-112024048 Earth Kasha Threat Actor Campaign |  |  |  |
|  | CMTX-P-112024814 Cumulative Suspicious Domains--ALERT3 |  |  |  |
|  | CMTX-I-388112024 Malicious Domain Typo-Squatting CBI Domain used by Threat Actors |  |  |  |
|  | CMTX-P-112024324 PlugX Malware Campaign |  |  |  |
|  | CMTX-I-981112024 Malicious Sub-Domains- Possibly Phishing |  |  |  |
|  | CMTX-P-112024904 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024804 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-I-355112024 CrimsonRAT- APT36 campaign |  |  |  |
|  | CMTX-P112024605 ACTIVE EXPLOITATION OF A CRITICAL FLAW (CVE-2023-28461) AFFECTING ARRAY NETWORK |  |  |  |
|  | CMTX-P112024705 Chinese APT "Earth Estries" Targeting Critical Infrastructure with New Attack Vectors and New Backdoor Malwares |  |  |  |
|  | CMTX-P-TL-1120243214 Notable Tunneling Tools leveraged by state sponsored/ ransomware actors |  |  |  |
|  | CMTX-I-770112024 AsyncRAT Malware |  |  |  |
|  | CMTX-I-070112024 Malicious Domain- Spear-Phishing |  |  |  |
|  | CMTX-P-112024394 PlugX Malware Campaign |  |  |  |
|  | CMTX-P-112024404 SHADOWPAD (POISONPLUG) Malware Campaign |  |  |  |
|  | CMTX-P-112024824 Cumulative Suspicious Domains--ALERT4 |  |  |  |
|  | TA-MAW-2024-11-18-002 RustDoor RAT Malware |  |  |  |
|  | TA-MAW-2024-11-18-003 AsyncRAT Malware |  |  |  |
|  | TA-APT-2024-11-18-006 CrimsonRAT- APT36 campaign |  |  |  |
|  | VA-2024-11-19-009 Threat Actors Exploiting RCE Vulnerability In The Palo Alto PAN-OS Management Interface |  |  |  |
|  | TA-PHI-2024-11-19-006 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2024-11-19-007 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2024-11-21-010 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-TAG-2024-11-21-002 Threat Group Insikt aka TAG-110 |  |  |  |
|  | TA-APT-2024-11-21-009 CrimsonRAT- APT36 campaign |  |  |  |
|  | TA-MAW-2024-11-21-005 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-APT-2024-11-21-010 APT SideCopy |  |  |  |
|  | TA-MAW-2024-11-21-006 Threat Actor FakeBat campaign |  |  |  |
|  | TA-MAW-2024-11-21-007 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-RAN-2024-11-22-005 Lockbit 3.0 Ransomware |  |  |  |
|  | TA-TAG-2024-11-25-003 Earth Kasha Threat Actor |  |  |  |
|  | TA-PHI-2024-11-25-011 Phishing Attack |  |  |  |
|  | TA-MAW-2024-11-25-008 PXA Stealer |  |  |  |
|  | TA-PHI-2024-11-25-012 Malicious Domains used by Threat Actors |  |  |  |
|  | TA-RAN-2024-11-25-006 Helldown Ransomware |  |  |  |
|  | TA-MAW-2024-11-25-009 ShadowPad Campaign Targeting Indian Energy Sector |  |  |  |
|  | TA-PHI-2024-11-26-013 Phishing Attack |  |  |  |
|  | TA-MAW-2024-11-26-009 Shadowpad Malware |  |  |  |
|  | TA-MAW-2024-11-26-010 Malicious IoCs |  |  |  |
|  | TA-MAW-2024-11-26-011 Malicious IoC Targeting Telecom Sector |  |  |  |
|  | TA-PHI-2024-11-26-014 Malicious Sub-Domains used by Threat Actors |  |  |  |
|  | TA-PHI-2024-11-26-015 Malicious Domains Typo-Squatting CBI Domain used by Threat Actors |  |  |  |
|  | TA-MAW-2024-11-27-012 Weekly Mirai Activity Report |  |  |  |
|  | TA-PHI-2024-11-27-016 CAPTCHA-Gated Phishing Pages Leveraged to conduct Financially Motivated Attacks |  |  |  |
|  | TA-APT-2024-11-27-011 APT SideCopy |  |  |  |
|  | VA-2024-11-27-012 Critical Vulnerabilities in Multiple Products |  |  |  |
|  | VA-2024-11-28-013 Exploitation of a Critical Flaw (CVE-2024-20481) Affecting Cisco Firepower Threat Defense (FTD) Software & Cisco Adaptive Security Appliance (ASA) Software |  |  |  |
|  | TA-PHI-2024-11-28-017 Phishing Attack |  |  |  |
|  | TA-APT-2024-11-28-012 APT Earth Estries |  |  |  |
|  | VA-2024-11-28-014 ACTIVE EXPLOITATION OF A CRITICAL FLAW (CVE-2023-28461) AFFECTING ARRAY NETWORK |  |  |  |
|  | TA-MAW-2024-11-28-013 Malicious IOCs Targeting Critical Sectors |  |  |  |
|  | TA-MAW-2024-11-29-014 Notable Tunneling Tools Leveraged by State Sponsored/ Ransomware Actors |  |  |  |
|  | TA-MAW-2024-11-29-015 AsyncRAT Malware |  |  |  |
|  | VA-2024-11-29-015 Threat Actors Operation Lunar Peek Activity to Exploit Vulnerabilities in Palo Alto Networks |  |  |  |